ABSTRACT

In an apparatus and a method for generating and verifying an identity based blind signature by using bilinear parings, a trust authority generates system parameters and selects a master key. Further, the trust authority generates a private key by using a signer's identity and the master key. The signer computes a commitment and sends the commitment to the user. The user blinds a message and sends the blinded message to the signer. The signer signs the blinded message and sends the signed message to the user. Thereafter, the user unblinds the signed message and then verifies the signature.